Basu 1-1

IN THE CLAIMS:

1. (Currently Amended) A system including a processor, and a collection of resources interacting with said processor, said resources including at least a memory and a library of executable modules that are supported by an operating system, the improvement comprising:

a plurality of processing stacks for dividing the system's computing environment into an unprotected portion and a protected portion, where the protected portion is protected from interloping processes in accord with an administratively specified schema, by mediating interactions between executing processes within said system and said resources, each of said stacks including a predefined set of at least one mediation module that processes ~~an applied signal~~ a request by at least one of said executing processes, which request is to be applied a resource of said collection of resources to form a signal, if appropriate pursuant to and in accord with such schema, that is applied to said resource of said collection of resources; and

a service director module that intercepts requests of different types that are directed to said resources, classifies said requests in accordance with said types of said requests, each different one of said resources being responsive to requests of a different type, and directs said requests to different ones of said processing stacks, based on said classifying.

2. (Original) The system of claim **1** wherein said at least one resource to which said signal is applied develops an output signal that is accepted by said at least one mediation module.

3. (Original) The system of claim **1**, wherein at least one processing stack of said plurality of processing stacks comprises an ordered sequence of at least two mediation modules.

4. (Previously Presented) The system of claim **1**, wherein said service director receives a request from an application that is active on said system and applies said request to said at least one mediation module.

5. (Original) The system of claim **4**, wherein said mediation module receives a return signal from said at least one resource of said collection of resources, processes said return signal to form a processed return signal, and sends said processed return signal to said application.

6. (Original) The system of claim **5** wherein said at least one resource of said collection of resources sends said processed return signal via said service director.

7. (Original) The system of claim **1**, wherein said at least one mediation module is based upon a chosen security policy.

8. (Original) The system of claim **1**, wherein said at least one mediation module in said processing stack performs encryption.

9. (Original) The system of claim **1**, wherein said mediation module is a namespace manager.

10. (Original) The system of claim **1**, wherein said mediation module performs authentication.

11. (Original) The system of claim **1** wherein said mediation module is a secure file system.

12. (Original) The system of claim **1**, wherein said service director includes:

a service request classifier that classifies a received service request; and

a processing stack selector that selects a processing stack based upon said classification, and communicates said service request to said selected processing stack.

Basu 1-1

13. (Original) The system of claim **1**, wherein said service director includes a service request classifier that classifies a service request based upon the type of service request and arguments of the service request.

14. (Original) The system of claim **1** further comprising a connection to a network.

15. (Original) The system of claim **14** wherein said connection is secure.

16. (Original) The system of claim **14**, wherein said network is a virtual private network.

17. (Original) The system of claim **16** wherein said connection is secured.

18. (Original) The system of claim **17** wherein said connection is secured through encryption.

19. (Original) The system of claim **1** further comprising a compliance supervisor that is coupled to said processing stacks, and to said service director, and is adapted for receiving security policy information from outside said system.

20. (Original) The system of claim **19**, wherein said compliance supervisor receives said security policy information from a virtual private network.

21. (Original) The system of claim **19**, wherein said compliance supervisor includes a processing stack modifier that modifies said processing stack based upon a received security policy.

22. (Original) The system of claim **19**, wherein said compliance supervisor includes a processing stack creator that creates a processing stack based upon said security policy.

Basu 1-1

23. (Original) The system of claim **1**, wherein said at least one mediation module includes at least one authentication code retriever that retrieves an authentication code and a validation system that validates said service request against said authentication code.

24. (Original) The system of claim **1** wherein said operating system includes means to prevent implication of an operating system breach from an administrative user breach.

25. (Original) The system of claim **1** wherein said service director and said processing stacks are embedded in a loadable library of C language executable modules.

26. (Original) The system of claim **1** further comprising a read-only program store that is read by said system upon boot-up.

27. (Currently Amended) A system including a processor, and a collection of resources interacting with said processor, said resources including at least a memory and a library of executable modules that are supported by an operating system, the improvement comprising:

a plurality of processing stacks, each including a predefined set of at least one mediation module that processes an applied signal to form a signal that is applied to said at least one resource of said collection of resources;

a service director module that intercepts requests of different types that are directed to said resources, classifies said requests in accordance with said types of said requests, each different one of said resources being responsive to requests of a different type, and directs said requests to different ones of said processing stacks, based on said classifying; and

a read-only program store that is read by said system upon boot-up;

~~The system of claim 26,~~ wherein said system includes an operating system, and said read-only program store contains a program module for verifying the operating

system, and authentication program modules for authenticating software present in said memory of said system.

28. (Original) The system of claim **27** where said software that is authenticated by said authentication program modules includes software that forms an operating system of said system.

29. (Original) The system of claim **28** where said authentication program modules develop a cryptographic hash of software to be authenticated.

30. (Previously Presented) A storage medium that stores a control routine for use by a system to assure security of said system, the control routine including instructions that, when said storage medium is coupled to said system, the instructions are adapted to:

boot said system with an authenticated operating system (AOS) located on said storage medium;

verify~~ing~~ an operating system of said system that is resident on said system (VOS);

transfer~~ring~~ control of said system from said AOS to said VOS when said VOS is verified, said transfer being sufficiently effective to allow intended operation of said system with said storage medium being decoupled from said system.

31. (Previously presented) The storage medium of claim **30**, wherein said instructions, when they boot said system, verify said operating system of said system by reading executable modules of said operating system of said system, determining a cryptographic hash for said executable modules, and comparing said cryptographic hash to a known value.

32. (Original) The storage medium of claim **30** where said control routine further includes steps for:

verifying software that implements a reverse sandbox on said system; and

transferring control of said standalone host to said reverse sandboxing software.

33. (Original) The storage medium of claim **30** further comprising reverse sandbox software to be installed in said system.

34. (Original) The storage medium of claim **33** wherein said reverse sandbox software includes a service director, a compliance supervisor, and a processing stack including at least one mediation module.